NATIONAL RESERVE BANK OF TONGA

Prudential Banking Standard No. 14 - 2021

OPERATIONAL RISK MANAGEMENT

INTRODUCTION

1. This Prudential Banking Standard is established under Section 20(3) of the Banking Act 2020 (the Act) and sets out the minimum standards which licensed financial institutions (Banks) operating in Tonga should adopt for the identification and management of operational risk.

2. In preparing this Prudential Banking Standard, reference has been made to the recommendations of the Basel Committee on Banking Supervision and other international sound practices and standards.

3. Operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events." Operational risk event types that have the potential to result in losses include:

   a) internal and external fraud;

   b) employment practices and workplace safety issues;

   c) failure to meet client obligations, or in the nature or design of products;

   d) damage to physical assets;

   e) business disruption and system failures;

   f) transaction processing and/or process management failures; and

   g) legal risk

OBJECTIVE

4. The objective of this Prudential Banking Standard is to ensure that each Bank has in place a comprehensive and effective operational risk management framework that is commensurate with the size, complexity, nature and scale of its operations.

5. Effective management of Operational Risk is integral to the nature of business the Banks perform and to its

roles as financial intermediaries. Although Operational Risk is not new, deregulation and globalization of financial services, together with growing sophistication of financial technology, and new business activities, are making Bank's operational risk more complex.

6. This Prudential Banking Standard is developed to outline the Reserve Bank's minimum requirements for the operational risk management framework of Banks, licensed to conduct banking business. In developing this Prudential Banking Standard, the Reserve Bank recognizes the differences in approaches to the management of operational risk.

ESTABLISHMENT OF AN OPERATIONAL RISK MANAGEMENT FRAMEWORK

Operational Risk Management Framework

7. Each Bank is required to establish a comprehensive and effective Operational Risk Management Framework (ORMF). This is the responsibility of the Board of Directors and the Senior Management. Risk management is the process of identifying, assessing, controlling and monitoring inherent operational risk in the conduct of banking business.

8. The ORMF is the totality of systems, structures, processes and people that address the operational risk management process. The ORMF sets the scope for the entire operational risk management process and determines how the process can be established and maintained within the Bank. The Framework consists of a fully documented Operational Risk Management Policy and Operational Risk Management Strategy.

Operational Risk Management Policy

9. In establishing the ORMF, each Bank is required to document its policy on managing operational risk. The policy is to ensure that the Banks approach to Operational Risk Management will cover operational risk management standards and objectives for all key underlying business and support processes.

10. 10. The documented Operational Risk Management Policy must be Board approved and appropriately designed for the size, nature, complexity and scale of risk and activity undertaken. The policy must reflect the internal and external environment within which each Bank's activities take place.

11. The Policy must be clearly communicated to all employees on a regular basis, to ensure that it is fully understood by the people responsible for managing these risks; and awareness levels are maintained and are consistently applied. All employees are to be regularly briefed on the "Three Lines of Defense" and their role.

11.1 the first line of defence is business line management. This means that sound operational risk governance will recognise that business line management is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.

11.2 A functionally independent operational risk function is typically the second line of defence, generally complementing the business line's operational risk management activities. The degree of independence of this function will differ among Banks. For small Banks, independence may be achieved through separation of duties and independent review of processes and functions. In larger Banks, this function will have a reporting structure independent of the risk generating business lines and will be responsible for the design,

maintenance and ongoing development of the operational risk framework within the Bank. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the operational risk function is to challenge the business lines' inputs to, and outputs from, the Bank's risk management, risk measurement and reporting systems. This function should have a sufficient number compared to the size of the Bank, and personnel skilled in the management of operational risk to effectively address its many responsibilities.

11.3 The third line of defence is an independent review and challenge of the Bank's operational risk management controls, processes and systems. Those performing these reviews must be competent and appropriately trained and not involved in the development, implementation and operation of the Framework. This review may be done by audit or by staff independent of the process or system under review, but may also involve suitably qualified external parties.

12. The Policy must facilitate the monitoring, measurement and management of such activities and needs to be subject to regular review and update to ensure they continue to reflect the environment within which the Banks operate.

13. The areas, at a minimum, that Operational Risk Management Policies should cover includes:

a) human resources;

b) internal controls;

c) compliance;

d) administration;

e) internal audit;

f) information technology/CyberSecurity

g) business continuity planning;

h) fraud;

i) new product development/change management;

j) related party, intra-group and conglomerate activities; and

k) outsourcing.

Operational Risk Management Strategy

14. The establishment of a successful framework also includes the development of strategies for Banks. This could be separately documented or contained within the Operational Risk Management Policy.

15. The Reserve Bank requires each Bank to develop an Operational Risk Management Strategy (ORMS) that is

documented, easily understood, auditable, accessible to all staff and reflective of the size, complexity and nature of the Bank's operational risk profile and exposure.

16. To establish an effective ORMS, the Banks need to identify stakeholders involved and what is required of them. This facilitates the identification of key business drivers and objectives.

17. In developing its strategy, each Bank should consider its strategic challenges in delivering those objectives and the consequences of not doing so. The ORMS should be reviewed continuously.

GOVERNANCE OF OPERATIONAL RISK MANAGEMENT

Organizational Structure for Operational Risk Management

18. Each Bank is required to define an organizational structure for operational risk management and clearly communicate individual roles and responsibilities and reporting lines. All operational risk management activities must be clearly understood and executed.

19. Whilst the ultimate responsibility for operational risk management resides with the Board, it is essential that:

    a) staff of the Bank understand their individual role in the risk management process clearly; and

    b) a proactive risk culture is created to support the identification and reporting of operational risk related issues to relevant parties.

Role and Responsibilities of Board

20. The Board of a Bank is required to:

    a) recognise operational risk as a distinct risk category;

    b) recognise the major operational risks inherent in its business and understand the risk management framework for this;

    c) approve and review a risk appetite for operational risk that articulates the nature, types, and levels of operational risk that the Board is willing to assume;

    d) approve assigned authority, responsibility and reporting relationship developed by Senior Management;

    e) receive updated reports from the Operational Risk Committee (OPCO) that enable it to understand the overall risk profile of the institution, in relation to the set risk appetite, and focus on the material and strategic implications;

    f) ensure that Senior Management is actively monitoring the effectiveness of risk controls, where such review should be carried out at least once a year;

    g) ensure that the operational risk management framework is subject to an effective and comprehensive review by the internal audit unit.

h) Approve the regularly reviewed Operational Risk Mangement Framework, Policy and Procedures

21. For branch operations in Tonga, the Board of each Bank is required to declare who is delegated responsibility for the oversight of operational risk in the Tonga branch through formalized Terms of Reference (TOR) or Charter, which should be regularly reviewed.

Role and Responsibility of Senior Management

22. Senior Management should ensure the ORMF approved by the Board is implemented consistently throughout the Bank, and all levels of staff should understand their responsibilities with respect to operational risk management.

23. Senior Management of each Bank is required to:

a) develop, implement and verify detailed policies and procedures for managing operational risk in all business activities, processes and systems;

b) ensure implementation of an effective operational risk management process;

c) upon approval of the Board, clearly assign authority, responsibility and reporting relationship for the Bank to facilitate decision-making and ensure accountability;

d) communicate clearly the operational risk management policy to staff across all risk areas within Bank's that incur material operational risks;

e) report comprehensively on operational risk management program to the Board on a timely basis; and

f) notify the Board of material changes or exceptions from established policies and procedures that could affect the operational risk management framework.

Independent Operational Risk Management Function (OPCO)

24. The Banks should, at a minimum, establish an Independent Operational Risk Management Function. The role of this Function is to design, implement and continuously develop the Bank's Operational Risk Management Framework and to assist Senior Management in meeting their responsibility for understanding and managing operational risk.

25. The Independent Operational Risk Management Function should at a minimum:

a) establish, maintain and monitor compliance arrangements, including processes and procedures that ensure compliance with the operational risk management framework;

b) define and document all roles, responsibilities and functions pertaining to the management of operational risk;

c) ensure consistent status and timely reporting to the Board and Senior Management;

d) design and implement a monitoring and reporting system for operational risk;

e) identify and monitor emerging trends and issues; and

f) ensure consistent liaison with internal and external audit.

ESTABLISHMENT OF RISK MANAGEMENT PROCESS

Risk Identification, Measurement and Assessment

26. Each Bank is required to establish risk identification processes. These should focus on both current and future operational risks. The operational risk identification process should consider:

a) the full spectrum of potential operational risks;

b) the internal and external environment in which each Bank operates;

c) the Bank's strategic objectives;

d) the products and services the Bank provides;

e) the Bank's unique circumstances;

f) the root causes and influencing factors of operational risk; and

g) the internal and external change and pace of that change.

27. The internal environment includes each Bank's structure, activities, quality of staff, organisational changes, employee turnover and its products and services. The external environment includes technological advances, changes in industry and other market information that affects the achievement of the Bank's objectives.

28. Risk identification should consider potential causes of operational risks, such as transaction processing, sales practices, management processes, human resources, vendors and suppliers, technology, external environment, disasters, unauthorized/criminal activities and political pressure

29. The risk identification process should employ tools and processes to ensure that the full spectrum of potential operational risks is captured. These include the use of key risk indicators, risk and compliance registers, risk maps and other tools.

Risk Mitigation and Controls

30. Each Bank must have appropriate control mechanisms in place to mitigate and control the identified risks. This is essential for effective operational risk management. Risk mitigation and control at a minimum should

include:

a) establishing Board approved policies, processes and procedures to control and or mitigate material operational risks;

b) ensuring that established control processes and procedures have in place a system for ensuring compliance;

c) the use of appropriate procedures to control and/or mitigate, or bear all material risks identified. For those risks that cannot be controlled, the Bank should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely;

d) clear and effective internal control system in place with clear assignment of roles and responsibilities, appropriate segregation of duties, to avoid conflicts of interest;

e) assurance of the effectiveness and appropriateness of controls in relation to risks identified;

f) identification of areas of potential conflict which should be subject to independent monitoring and review by Senior Management; and

g) use of risk mitigation tools, models or programmes to reduce the exposure to, or frequency and /or severity of risks events.

Monitoring and Reporting Risk

31. The Senior Management of each Bank is required to implement a system to monitor operational risk profiles, material exposures, incidents and breaches, losses and key risk indicators on an on-going basis.

32. Senior Management is also required to incorporate regular reporting/register of operational exposures, loss experience, group risk, specialist functions and internal through its operational risk organisational structure and ultimately to the Board.

33. The reports should at the least contain internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports should fully reflect any identified problem areas and should prompt timely and corrective action on outstanding issues.

34. Reports should be discussed within the Operational Risk Function Executive Committee meetings on a monthly basis and distributed to appropriate levels of management and areas of the Bank relevant to the issues/risks/deficiencies being reported. A timeline given for their proactive measures to address the issues/risks/deficiency. Finalized risk report to be reported to Board.

35. Senior Management should establish an escalation process through the operational risk organizational structure for reporting and regularly monitor the timeliness, accuracy and relevance of reporting systems, and internal controls to ensure the usefulness and reliability of reports.

KEY OPERATIONAL RISK AREAS

Human Resources

36. The management of human resources and employee behavior can become a major source of operational risk. Poorly trained back-up employees or overworked employees may inadvertently expose a Bank to operational risk (for example, via processing errors). Understanding of the mandate, confidence in and respect for the institution as well as adherence to the Bank's policies and strategies are key for effective use of human resources. In addition, the continuous availability of its employees, or the Bank's ability to replace them as they leave, can influence its ability to recover from interruptions to the continuity of its operations. Therefore, the Bank can realize significant improvements in its control of operational risk and reduce exposure if it invests time and money in creating an appropriate risk culture, in which employees are aware of operational risks and are encouraged to learn from their mistakes.

37. Each Bank must develop a Board approved Human Resource policy that sets out its approach to human resource management. The policy must ensure that the Bank's business activities are conducted by competent staff who have a well-grounded understanding of all types of risk involved in their activities, and have sufficient knowledge, and regular training and expertise to carry out their responsibilities.

38. The Bank shall include in induction and regular training an awareness programme on ALL Policies and procedures of the Bank.

39. Banks are to develop a Whistleblower policy. To promote an environment where staff feels free, confident and encouraged to reveal any serious concerns that they may have about the conduct of employees at all levels in the Bank, rather than overlooking a problem or "blowing the whistle" outside the Bank, without fear of victimization, subsequent discrimination of being disadvantaged in any way.

40. The human resource management program should encompass:
    a) an ongoing, appropriate and effective process to attract and retain a sufficient number of qualified personnel to achieve the Bank's business objectives and implement its business strategy and business plans;

    b) defined and prudent levels of decision-making authority;

    c) segregation of incompatible functional responsibilities;

    d) separation of duties between front and back offices of the Bank;

    e) clear communication to personnel of their responsibilities; In the case of Bank introducing new products, change in management or structure. All staff will be disclosed in clear communication method well in advance to effective date of any change in management or organizational structure or introduction of new products.

    f) effective supervision of personnel; clearly providing redemption steps when personnel fail to meet job description or breach internal procedures. And also ensuring that functions are sufficiently covered when part of staff is on leave (strong back-up system)

g) background checks for personnel working in sensitive or high-risk areas.

Internal Controls

41. Each Bank must have in place internal controls that are adequate for the size and complexity of their business. These should include clear arrangements for delegating authority and responsibility, separation of the functions that involve committing the Bank, paying away its funds and accounting for its assets and liabilities, reconciliation of these processes and safeguarding the Bank's assets.

    The internal control environment should be subject to appropriate independent internal audit and compliance functions to test adherence to these controls as well as applicable laws and regulations, on at least an annual basis, and whenever deemed necessary by the Board.

    Bank units should regularly update internal controls and procedures to ensure current practice is documented for verification and regular review by the internal auditor and compliance functions.

Compliance

42. Each Bank should affirm the importance of the compliance function by appointing senior personnel, or an appropriate unit to oversee compliance issues.

43. Each Bank should ensure that compliance officers are equipped with the necessary skills and expertise in line with the level of complexity of the Bank's products and activities.

44. Each Bank should ensure that compliance personnel, among other responsibilities, provide advice and training on regulatory requirements and standards of professional conduct to staff, and conduct periodic reviews to assess compliance with policies, procedures, and regulatory requirements.

45. Compliance personnel should furnish reports to the Board on a periodic basis to provide information on compliance risk. Any violations of law or regulation, and any and all correspondence from the Reserve Bank dealing with noncompliance should be presented to the Board. The Board should ensure that corrective action is taken and should require amendments to policies and procedures, internal controls, and processes to prevent recurrence of such deficiencies.

Administration

46. Administrative risk refers to the risk of a Bank incurring a loss due to the neglect by officers and employees in conducting the administrative work of the Bank, accidents in the course of that work, or breaches of laws, regulations or internal procedural requirements in the course of the administrative work process.

47. The development and establishment of a system for managing administrative risks is extremely important from the viewpoint of ensuring the soundness and appropriateness of a Bank's business. Therefore, the Bank's Board and Senior Management must take the initiative in developing and establishing such a system[1].

[1] For purposes of this Prudential Banking Standard, Senior Management includes those persons appointed by the Board to conduct the significant day-to-day operations of the Bank. This would include the Chief Executive Officer, General Manager, senior managers, senior executives, or persons performing equivalent functions, regardless of formal title.

48. The system must ensure that the roles and responsibilities of the Bank's management are being appropriately performed, and specifically that the management is appropriately implementing:
    a) policy development;

    b) development of internal rules and organizational frameworks; and

    c) development of a system for assessment and improvement activities.

49. If a problem is recognized, it is necessary to examine which of the above-mentioned elements are absent or insufficient, thus causing the problem, and to review findings thereof through dialogue between the risk management function and the Board and Senior Management.

50. If the Bank's Senior Management fails to recognize weaknesses or problems, it is also necessary for the Board to examine in particular the possibility that the Internal Control System is not functioning effectively and to take steps to remedy the situation.

51. The Board should periodically review the status of any remedial measures with regard to those issues pointed out on the occasion of the last internal review that are not minor and determine whether or not effective improvement measures have been developed and implemented.

Internal Audit

52. Each Bank should regularly check and evaluate how well its operational risk management system operates. The internal auditor should have in place a well-defined scope of work which is regularly reviewed and approved by the Board.

53. The Bank's internal audit function should supervise the implementation of operational risk management policies and independently evaluate new operational risk management policies, processes and specific procedures.

54. The internal audit function should report to the Board of Directors, directly or through a designated Board committee, the evaluation results of operational risk management system.

55. The Reserve Bank may request the external auditor of the Bank, or an appropriate external expert, to provide an assessment of the risk management processes.

Information Technology

56. Each Bank should have adequate information systems for effective management and control of all aspects of its operations. This should be commensurate with the complexity and diversity of its operations. Systems support and operational capabilities should accommodate the activities in which it engages.

    Each Bank should ensure regular updated security systems in place with a strong back-up system. Cyber risk management minimum requirements are covered under the Cyber security Risk Management Prudential Banking Standard. In an effort to minimize information system failure or disruption, IT team should lead a regular IT awareness programme. This will include maintaining a risk register to pass on to ALCO, regular

update to ALL staff on latest information on viruses and clear steps to securing the information system of the Bank.

57. Each Bank should deploy the necessary resources to develop and maintain the operations and systems supporting its activities.

58. Each Bank should report on its information systems operations and this should be sent to management for review.

59. Each Bank should ensure that adequate policies and procedures are established in authorising, administering and regularly reviewing user access to the network. As a general principle, developers should not have access to the IT production environment.

60. Each Bank should ensure that its IT unit facilitate with respective personnel the induction, awareness, education, and training in business information security.

Business Continuity Management

61. Each Bank is required to develop a Board approved Business Continuity Management (BCM) Policy. This would allow the Bank to identify, assess and manage potential business continuity risks to be able to meet its financial and service obligations.

62. Each Bank should consider in its BCM policy different types of likely scenarios to which it may be vulnerable, and identify critical business functions including those where there is dependence on external vendors or other third parties for which rapid resumption would be essential.

63. At a minimum, the Bank's BCM should include Business Impact Analysis (BIA), Risk Assessment, Recovery Strategy, Business Continuity Plan (BCP) and Disaster Recovery Plan for IT (DRP), and a regular review, testing and maintenance of the BCM.

Business Impact Analysis

64. Each Bank is required to ascertain its key business functions, resources and infrastructure and the maximum downtimes for these before a disruption has a material impact on its operation.

65. The BIA must include mapping internal processes and/or their interrelationships and should involve active participation by the Senior Management. It ensures an adequate representation from all potentially impacted business functions within the Bank's.

66. At a minimum, the BIA should include:

    a) assessment of the likely disruption to business operations in the event of a loss of a critical business process for defined periods of time;

    b) determination of alternative sources of information/services available;

    c) assessment of the financial and non-financial costs during business disruption and the probable recovery

time for each critical business; and

d) identification of specific threats to the critical business processes, including assessment of geographic location of installations and the prevailing conditions.

Business Continuity Plan and Disaster Recovery Plan for IT Recovery

67. Each Bank is required to develop a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). The BCP and DRP will enable a Bank to:

a) respond to a material disruption to normal business operations and critical IT systems;

b) recover and continue critical business functions and IT systems in an orderly manner;

c) plan to return business and IT systems to normal operations after material disruption; and

d) consider wide area disruptions.

68. The BCP and DRP of each Bank should, at a minimum include:

a) the detailed procedures to be followed in response to a material disruption to normal business operations and critical IT systems;

b) a list of all resources needed and a plan to efficiently utilize these resources in order to run IT and normal operations in the event the primary operational site is unavailable;

c) a communication and public relations plan for contacting key internal and external stakeholders if the institution's BCP or DRP is invoked;

d) training and seminars to promote understanding of the roles, duties and responsibilities of the Bank's employees and persons relevant to the BCP or DRP;

e) outsourcing arrangements or contract with a critical third-party service provider should address business continuity plan and IT recovery; and

f) important information about an institution's alternate operation site for the recovery of business and/or IT operations if this forms part of the institution's BCP/DRP.

g) Availability of a back-up server to ensure minimum impact of any form of disruption.

69. Off-site copies of the BCP must be kept by a number of responsible senior managers who have designated responsibilities in terms of the BCP and should also be available at the alternate recovery site, if applicable.

Review, Maintenance and Testing of BCM

70. Banks should set clear procedures, and designate responsible persons to regularly, review, test and maintain the BCM components.

71. Banks should stipulate appropriate and regular testing of the BCM by simulating real life situations and upon completion, the test results should be assessed by an internal auditor.

Recovery Strategy

72. Each Bank is required to develop and implement a Recovery Strategy based on the results of BIA and Risk Assessment. This may involve the use of the Bank's alternate operational site. A key risk to be mitigated when using an alternate operational site is that the primary operational site and alternate operational site are not unavailable simultaneously due to close physical proximity and/or shared critical infrastructure.

73. Banks should consider critical data and specialist software, covering frequency of update, remoteness from the prime site, processing capability, responsibility for back-ups and the maintenance of adequate documentation on how to use the back-ups when establishing appropriate off-site storage.

Fraud

74. Each Bank should have in place proper financial accounting controls and adequate monitoring. It should include "red flags" that can quickly identify potential fraudulent activities.

75. Each Bank should ensure that regular management reports should cover not only amounts and types of fraud, but the trend analysis of the particular fraud.

76. The Reserve Bank may undertake a risk assessment and where necessary, seek expert support.

77. Each Bank should ensure that staff are trained on the potential sources of fraud and controls used in fraud risk management.

New Product Development

78. Before undertaking any new line of business, determining to introduce any new products or instruments, utilizing any new business strategy, or any change in Management the Bank's Board must approve such proposals after a comprehensive analysis, review, and evaluation of the risks involved. Such approval must be based on a determination by the Board that undertaking the proposed new business activity, or the use of the proposed new product, instrument, or business strategy, is in the best interest of the Bank and that there is an effective process in place to manage any risks involved. The results of the Board's analysis, review, evaluation and determination must be documented in the Board's minutes.

    Materials for review must consist of:

    a. A Feasibility Study including but not limited to:

        i. a description of the new business activity, product, instrument or strategy;

        ii. identification of the resources required to establish and maintain sound and effective management of the new business activity, product, instrument or strategy, including management of the risks involved

iii. analysis of the reasonableness of the proposed new business activity, product, instrument or strategy in relation to the Bank's overall financial condition and capital level;

iv. procedures to be used to measure, monitor, and control the risks of the proposed new business activity, product, instrument or strategy.

b. A submitted revised BCP and DRP to reflect consideration of any related risk from the proposed new line of business, determining to introduce any new products or instruments, utilizing any new business strategy

79. Banks are to inform The Reserve Bank on all new initiatives or significant changes 30 days before effective date. All related materials will be submitted to The Reserve Bank for their final endorsement for new products/new line of business.

Intra-Group or Conglomerate Activities

80. Each Bank should establish policies and procedures that address all dealings with related parties. This should cover operational risks that could arise from intra group or conglomerate activities. Where a Bank is part of a financial group, it must ensure that there are processes and procedures in place to ensure that operational risk is managed in an appropriate and integrated manner across the group.

81. Each Bank should properly document all policies relating to the activities it engages in with its related entities.

82. Policies and procedures should establish the requirement for staff to report directly to Senior Management and the Board any potential operational risk issues such as conflicts of interest that arise from intragroup and conglomerate activities.

83. Each Bank is required to report promptly to the Reserve Bank any operational risk issues that arises in the context of its intra group or conglomerate activities.

Outsourcing

84. Each Bank must develop a Board approved outsourcing policy that sets out its approach to outsourcing of material business activities, including a detailed framework for managing outsourcing arrangements.

    a. Material Business Activity would include outsourcing functions such as:
        i. Internal Audit Function
        ii. Information Technology Function
        iii. Back-Office Functions (Credit/Operations/Human Resource/Business Continuity Plan/Disaster Recovery Plan)

85. Banks must ensure that procedures are in place to ensure that all relevant business units of the Bank, are aware of and comply with the outsourcing policy.

86. Banks must ensure that all outsourcing arrangements are evidenced by a written, legally binding agreement, and this is to be submitted to The Reserve Bank for information and endorsement which must be executed before the outsourcing arrangement commences.

87. At a minimum, the agreement must address the following:

    a. the scope of the services to be supplied;
    b. commencement and end dates;
    c. provision for periodic review of arrangement;
    d. fee structure;
    e. performance requirements and service level agreements;
    f. audit and monitoring procedures;
    g. business continuity management;
    h. confidentiality, privacy and security of information;
    i. default and termination provisions;
    j. dispute resolution processes;
    k. liability and indemnity provisions;
    l. sub-contracting controls and monitoring; and
    m. insurance arrangements of the service provider.

88. An outsourcing agreement must include a clause that allows the Reserve Bank access to documentation and information related to the outsourcing arrangement, and to conduct on-site reviews of the service provider if the Reserve Bank considers this necessary to appropriately assess the risk of the outsourcing activity.

89. The service provider's BCP and DRP test results should be requested by Banks and the Reserve Bank when necessary that rely on the services outsourced. These documents should be reviewed and assessed to provide a level of assurance that the service provider's plans and practices are adequate.

90. Service providers should have adequate business continuity arrangements in place and this should form part of the "due diligence" process undertaken by Banks, when entering into an outsourcing arrangement.

91. Each Bank must consult with the Reserve Bank prior to entering agreements to outsource material business activities to service providers, who conduct their activities within and outside Tonga. An outsourcing agreement must include a clause which allows Reserve Bank access to the Service Providers documentation and processes related to the outsourcing arrangement.

The Reserve Bank will have a right to request any policy, agreement, and any other report from third party relating to dealings with Bank.

The Bank or third party will inform The Reserve Bank of any identified issue relating to their working relationship with Bank.

DISCLOSURE

92. Each Bank must disclose its operational risk management framework in accordance with this Prudential Banking Standard. The disclosure should summarize how the Board and Senior Management assess and manage the operational risk of the Bank, and should contain information sufficient to allow stakeholders to determine whether the Bank identifies, assesses, monitors and controls/mitigates operational risk effectively.

OVERSIGHT OF THE RESERVE BANK

93. For the purpose of this Statement, all Banks are required to provide to the Reserve Bank its initial ORMF including; its ORMP and ORMS within 30 calendar days from the date of implementation, and thereinafter before end of December each year. Furthermore, each Bank must provide a copy of the same whenever amendments are made, and this must be submitted to the Reserve Bank within 30 days of Board approval.

94. Each Bank is required to report to the Reserve Bank, any material operational risk incident no later than 24 hours of its occurrence. (**Annex 1**)

COMPLIANCE WITH PRUDENTIAL BANKING STANDARD 14

95. This statement is effective from 1st July 2021. Non-compliance with the requirements of this Prudential Banking Standard will be subject to corrective actions as provided under section 39 of the Banking Act 2020 and the administrative penalties outlined in Prudential Banking Standard No.3 Administrative Penalties.

EFFECTIVE DATE

96. This guideline applies to Banks licensed under the Act and will be effective from 1st July, 2021.